Installez et configurez un Module de services de puissance de feu sur une plate-forme ASA

Contenu

Introduction

Ce document décrit comment installer et configurer un module de la puissance de feu de Cisco (SFR) qui fonctionne sur une appliance de sécurité adaptable Cisco (ASA) et comment enregistrer le module SFR avec le centre de Gestion de Cisco FireSIGHT.

Conditions préalables

Conditions requises

Cisco recommande que votre rassemblement de système ces conditions requises avant que vous tentiez les procédures qui sont décrites dans ce document :

- Assurez-vous que vous avez au moins 3GB de l'espace libre sur le lecteur flash (disk0), en plus de la taille du logiciel de démarrage.
- Assurez-vous que vous avez accès au mode d'exécution privilégié. Afin d'accéder au mode d'exécution privilégié, sélectionnez la commande d'**enable** dans le CLI. Si un mot de passe n'était pas placé, alors appuyez sur **entrent** :

```
ciscoasa> enablePassword:ciscoasa#
```

Composants utilisés

Afin d'installer les services de puissance de feu sur Cisco ASA, ces composants sont exigés :

- Version de logiciel 9.2.2 de Cisco ASA ou plus tard
- Plateformes 5512-X de Cisco ASA par 5555-X
- Version de logiciel 5.3.1 de puissance de feu ou plus tard

  Remarque: Si vous voulez installer des services de la puissance de feu (SFR) sur un module de matériel ASA 5585-X, lisez l'installation des services de la puissance de feu (SFR) sur le module de matériel ASA 5585-X.

Ces composants sont exigés au centre de Gestion de Cisco FireSIGHT :

- Version de logiciel 5.3.1 de puissance de feu ou plus tard
- Centre de Gestion de FireSIGHT FS2000, FS4000 ou appliance virtuelle

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le module de puissance de feu de Cisco ASA, également connu sous le nom d'ASA SFR, fournit les services de la deuxième génération de Pare-feu, comme :

- Système de prévention des intrusions de nouvelle génération (NGIPS)
- Visibilité d'application et contrôle (AVC)
- Filtrage des URL
- Protection avancée de malware (AMPÈRE)

  Remarque: Vous pouvez utiliser le module ASA SFR dans simple ou le mode de contexte multiple, et en mode conduit ou transparent.

Avant de commencer

Considérez ces informations importantes avant que vous tentiez les procédures qui sont décrites dans ce document :

- Si vous avez une stratégie de service active qui réoriente le trafic à un module averti du Système de prévention d'intrusion (IPS) /Context (la CX) (ce vous avez remplacé par l'ASA SFR), vous devez le retirer avant que vous configuriez la stratégie de service ASA SFR.

- Vous devez arrêter tous les autres modules logiciels qui fonctionnent actuellement. Un périphérique peut exécuter un module logiciel simple à la fois. Vous devez faire ceci de l'ASA CLI. Par exemple, ces commandes arrêtent et désinstallent le module logiciel IPS, et puis rechargent l'ASA :

  `ciscoasa# sw-module module ips shutdownciscoasa# sw-module module ips uninstallciscoasa# reload`Les commandes qui sont utilisées afin de retirer le module de la CX sont identiques, à moins que le mot clé de **cxsc** soit utilisé au lieu de l'**IPS** :

```
ciscoasa# sw-module module cxsc shutdownciscoasa# sw-module module cxsc uninstallciscoasa#
reload
```

- Quand vous réimagez un module, utilisez le même **arrêt** et **désinstallez les** commandes qui sont utilisées afin de retirer une vieille image SFR. Voici un exemple :

```
ciscoasa# sw-module module sfr uninstall
```

- Si le module ASA SFR est utilisé dans le mode de contexte multiple, exécutez les procédures qui sont décrites dans ce document dans l'espace d'exécution de système.

Conseil : Afin de déterminer le statut d'un module sur l'ASA, sélectionnez la commande de **show module**.

Installez

Cette section décrit comment installer le module SFR sur l'ASA et comment installer l'image de démarrage ASA SFR.

Installez le module SFR sur l'ASA

Terminez-vous ces étapes afin d'installer le module SFR sur l'ASA :

1. Téléchargez le logiciel système ASA SFR de Cisco.com à un HTTP, à un HTTPS, ou à un ftp server qui est accessible de l'interface de gestion ASA SFR.

2. Téléchargez l'image de démarrage au périphérique. Vous pouvez employer le Cisco Adaptive Security Device Manager (ASDM) ou l'ASA CLI afin de télécharger l'image de démarrage au périphérique. Remarque: Ne transférez pas le logiciel système ; il est téléchargé plus tard au lecteur semi-conducteur (disque transistorisé).Terminez-vous ces étapes afin de télécharger l'image de démarrage par l'intermédiaire de l'ASDM :

   Téléchargez l'image de démarrage à votre poste de travail, ou placez-la sur un serveur de FTP, TFTP, de HTTP, HTTPS, de server message block (PME), ou de Secure Copy (SCP).

   Choisissez les **outils > la gestion de fichiers** dans l'ASDM.

   Choisissez la commande appropriée de transfert de fichiers, *entre l'ordinateur local et l'éclair* ou *entre le serveur distant et l'éclair*.

   Virez le logiciel de démarrage sur le lecteur flash (disk0) sur l'ASA.Terminez-vous ces étapes afin de télécharger l'image de démarrage par l'intermédiaire de l'ASA CLI :

   Téléchargez l'image de démarrage sur un serveur de FTP, TFTP, de HTTP, ou HTTPS.

   Écrivez la Commande **COPY** dans le CLI afin de télécharger l'image de démarrage au lecteur flash.

   Voici un exemple qui utilise le protocole HTTP (remplacez le **<HTTP_Server>** par votre

adresse IP du serveur ou nom d'hôte) :

```
ciscoasa# copy http://<HTTP_SERVER>/asasfr-5500x-boot-5.3.1-152.img disk0:/asasfr-5500x-
boot-5.3.1-152.img
```

3. Sélectionnez cette commande afin de configurer l'emplacement d'image de démarrage ASA SFR dans le lecteur flash ASA :

```
ciscoasa# sw-module module sfr recover configure image disk0:/file_path
```
Voici un exemple :

```
ciscoasa# sw-module module sfr recover configure image disk0: /asasfr-5500x-boot-5.3.1-
152.img
```

4. Sélectionnez cette commande afin de charger l'image de démarrage ASA SFR :

```
ciscoasa# sw-module module sfr recover boot
```
Pendant ce temps, si vous activez **mettez au point le module-démarrage** sur l'ASA, ceux-ci met au point sont imprimés :

```
Mod-sfr 788> *** EVENT: Creating the Disk Image...
Mod-sfr 789> *** TIME: 05:50:26 UTC Jul 1 2014
Mod-sfr 790> ***
Mod-sfr 791> ***
Mod-sfr 792> *** EVENT: The module is being recovered.
Mod-sfr 793> *** TIME: 05:50:26 UTC Jul 1 2014
Mod-sfr 794> ***
...
Mod-sfr 795> ***
Mod-sfr 796> *** EVENT: Disk Image created successfully.
Mod-sfr 797> *** TIME: 05:53:06 UTC Jul 1 2014
Mod-sfr 798> ***
Mod-sfr 799> ***
Mod-sfr 800> *** EVENT: Start Parameters: Image: /mnt/disk0/vm/vm_3.img,
ISO: -cdrom /mnt/disk0
Mod-sfr 801> /asasfr-5500x-boot-5.3.1-152.img, Num CPUs: 6, RAM: 7659MB,
Mgmt MAC: A4:4C:11:29:
Mod-sfr 802> CC:FB, CP MAC: 00:00:00:04:00:01, HDD: -drive file=/dev/md0,
cache=none,if=virtio,
Mod-sfr 803> Dev
Mod-sfr 804> ***
Mod-sfr 805> *** EVENT: Start Parameters Continued: RegEx Shared Mem:
32MB, Cmd Op: r, Shared M
Mod-sfr 806> em Key: 8061, Shared Mem Size: 64, Log Pipe: /dev/ttyS0_vm3,
Sock: /dev/ttyS1_vm3,
Mod-sfr 807>  Mem-Path: -mem-path /hugepages
Mod-sfr 808> *** TIME: 05:53:06 UTC Jul 1 2014
Mod-sfr 809> ***
Mod-sfr 810> IVSHMEM: optarg is key=8061,64,unix:/tmp/nahanni, name is,
key is 8061, size is 6
...
Mod-sfr 239> Starting Advanced Configuration and Power Interface daemon:
acpid.
Mod-sfr 240> acpid: starting up with proc fs
Mod-sfr 241> acpid: opendir(/etc/acpi/events): No such file or directory
Mod-sfr 242> starting Busybox inetd: inetd... done.
Mod-sfr 243> Starting ntpd: done
Mod-sfr 244> Starting syslogd/klogd: done
Mod-sfr 245>
Cisco ASA SFR Boot Image 5.3.1
```

5. Attendez approximativement 5 à 15 minutes le module ASA SFR à initialiser, et puis pour ouvrir une session de console à l'image de démarrage opérationnelle ASA SFR.

Installez l'image de démarrage ASA SFR

Terminez-vous ces étapes afin d'installer la l'image de démarrage nouvellement installée ASA SFR :

1. La presse **entrent** après que vous ouvriez une session afin d'atteindre l'invite d'ouverture de connexion. Remarque: Le nom d'utilisateur par défaut est **admin**, et le mot de passe par défaut est **Admin123**.Voici un exemple :

   ```
   ciscoasa# session sfr consoleOpening console session with module sfr.Connected to module sfr. Escape character sequence is 'CTRL-^X'.Cisco ASA SFR Boot Image 5.3.1asasfr login: adminPassword: Admin123
   ```

   Conseil : Si le démarrage de module ASA SFR ne s'est pas terminé, la commande de session échoue et un message semble indiquer que le système ne peut pas se connecter au-dessus de TTYS1. Si ceci se produit, attente le démarrage de module à se terminer et essayer de nouveau.
2. Sélectionnez la **commande setup** afin de configurer le système de sorte que vous puissiez installer le module de logiciel système :

   ```
   asasfr-boot> setup                    Welcome to SFR Setup
   [hit Ctrl-C to abort]                   Default values are inside []
   ```

   Vous êtes alors incité pour ces informations :

   Nom d'hôte - Le nom d'hôte peut être jusqu'à 65 caractères alphanumériques, sans les espaces. On permet l'utilisation des traits d'union.

   Adresse réseau - L'adresse réseau peut être des adresses statiques d'ipv4 ou d'IPv6. Vous pouvez également utiliser le DHCP pour l'ipv4, ou la configuration automatique sans état d'IPv6.

   L'information DNS - Vous devez identifier au moins un serveur de Système de noms de domaine (DNS), et vous pouvez également placer le nom de domaine et rechercher le domaine.

   Les informations de NTP - Vous pouvez activer le Protocole NTP (Network Time Protocol) et configurer les serveurs de NTP afin de placer l'heure système.

3. Entrez dans le **système installent la** commande afin d'installer l'image du logiciel système :

   ```
   asasfr-boot >system install [noconfirm] url
   ```

   Incluez l'option de **noconfirm** si vous ne voulez pas répondre aux messages de confirmation. Remplacez le mot clé **URL** par l'emplacement du fichier **.package**. Voici un exemple :

   ```
   asasfr-boot >system install http:/<HTTP_SERVER>/asasfr-sys-5.3.1-152.pkgVerifyingDownloadingExtractingPackage Detail Description: Cisco ASA-FirePOWER 5.3.1-152 System Install Requires reboot: YesDo you want to continue with upgrade? [y]: yWarning: Please do not interrupt the process or turn off the system. Doing so might leave system in unusable state.UpgradingStarting upgrade process ...Populating new system imageReboot is required to complete the upgrade. Press 'Enter' to reboot the system.(press Enter)Broadcast message from root (ttyS1) (Mon Jun 23 09:28:38 2014):The system is going down for reboot NOW!Console session with module sfr terminated.
   ```

Remarque: Quand l'installation est complète, les réinitialisations de système. Accordez dix minutes ou plus pour l'installation composante d'application et pour les services ASA SFR pour commencer. La sortie de la commande de **sfr de show module** devrait indiquer que tous les processus sont **en hausse**.

Configurez

Cette section décrit comment configurer le logiciel de puissance de feu et le centre de Gestion de FireSIGHT, et comment réorienter le trafic au module SFR.

Configurez le logiciel de puissance de feu

Terminez-vous ces étapes afin de configurer le logiciel de puissance de feu :

1. Ouvrez une session au module ASA SFR. Remarque: Une invite d'ouverture de connexion différente apparaît maintenant parce que la procédure de connexion se produit sur un module plein-fonctionnel.Voici un exemple :

   ```
   ciscoasa# session sfrOpening command session with module sfr.Connected to module sfr.
   Escape character sequence is 'CTRL-^X'.Sourcefire ASA5555 v5.3.1 (build 152)Sourcefire3D
   login:
   ```
2. Ouvrez une session avec l'**admin** et le mot de passe **Sourcefire de** nom d'utilisateur.

3. Terminez-vous la configuration de système comme incitée, qui se produit dans cette commande :

   Lisez et recevez le contrat de licence utilisateur final (CLUF).

   Changez le mot de passe administrateur.

   Configurez l'adresse de gestion et les configurations de DN, comme incité. Remarque: Vous pouvez configurer des adresses de gestion d'ipv4 et d'IPv6.Voici un exemple :

   ```
   System initialization in progress. Please stand by. You must change the password for
   'admin' to continue. Enter new password: <new password>Confirm new password: <repeat
   password>You must configure the network to continue.You must configure at least one of IPv4
   or IPv6.Do you want to configure IPv4? (y/n) [y]: yDo you want to configure IPv6? (y/n)
   [n]:Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:Enter an IPv4 address for
   the management interface [192.168.45.45]:198.51.100.3Enter an IPv4 netmask for the
   management interface [255.255.255.0]: 255.255.255.0Enter the IPv4 default gateway for the
   management interface []: 198.51.100.1Enter a fully qualified hostname for this system
   [Sourcefire3D]: asasfr.example.comEnter a comma-separated list of DNS servers or 'none' []:
   198.51.100.15, 198.51.100.14Enter a comma-separated list of search domains or 'none'
   [example.net]: example.comIf your networking information has changed, you will need to
   reconnect.For HTTP Proxy configuration, run 'configure network http-proxy'
   ```
4. Attente le système pour se modifier.

Configurez le centre de Gestion de FireSIGHT

Afin de gérer un module et la stratégie de sécurité ASA SFR, vous devez [l'enregistrer avec un centre de Gestion de FireSIGHT](). Vous ne pouvez pas exécuter ces actions avec un centre de

Gestion de FireSIGHT :

- Configurez les interfaces de module ASA SFR
- Arrêté, la reprise, ou gèrent autrement les processus de module ASA SFR
- Créez les sauvegardes, ou restaurez les sauvegardes, derrière les périphériques de module ASA SFR
- Écrivez les règles de contrôle d'accès afin d'apparier le trafic avec l'utilisation des états de balise VLAN

Réorientez le trafic au module SFR

Afin de réorienter le trafic au module ASA SFR, vous devez créer une stratégie de service qui identifie le trafic spécifique. Terminez-vous ces étapes afin de réorienter le trafic à un module ASA SFR :

1. Sélectionnez le trafic qui devrait être identifié avec la **commande access-list**. Dans cet exemple, tout les trafic de toutes les interfaces est réorienté. Vous pouvez faire ceci pour le trafic spécifique aussi bien.

   ```
   ciscoasa(config)# access-list sfr_redirect extended permit ip any any
   ```
2. Créez un class-map afin d'apparier le trafic sur une liste d'accès :

   ```
   ciscoasa(config)# class-map sfrciscoasa(config-cmap)# match access-list sfr_redirect
   ```
3. Spécifiez le mode de déploiement. Vous pouvez configurer votre périphérique en mode (normal) passif (réservé au moniteur) ou intégré de déploiement. Remarque: Vous ne pouvez pas configurer un mode passif et le mode d'en ligne en même temps sur l'ASA. On permet seulement un type de stratégie de sécurité.Dans un déploiement intégré, après que le trafic peu désiré soit abandonné et toutes les autres actions qui sont appliquées par stratégie sont exécutés, le trafic est retourné à l'ASA pour une transformation plus ultérieure et une transmission finale. Cet exemple affiche comment créer un policy-map et configurer le module ASA SFR dans le mode intégré :

   ```
   ciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class sfrciscoasa(config-pmap-c)# sfr fail-open
   ```
   Dans un déploiement passif, une copie du trafic est envoyée au module de service SFR, mais elle n'est pas retournée à l'ASA. Le mode passif te permet pour visualiser les actions que le module SFR se serait terminées en vue de le trafic. Il te permet également pour évaluer le contenu du trafic, sans incidence au réseau.

   Si vous voulez configurer le module SFR en mode passif, utilisez le mot clé **réservé au moniteur** (suivant les indications de l'exemple suivant). Si vous n'incluez pas le mot clé, le trafic est introduit le mode intégré.

   ```
   ciscoasa(config-pmap-c)# sfr fail-open monitor-only
   ```
   Avertissement : Le mode **réservé au moniteur** ne permet pas au module de service SFR pour refuser ou bloquer le trafic malveillant.**Attention** : Il pourrait être possible de configurer une ASA en mode *réservé au moniteur* avec l'utilisation de la commande **réservée au moniteur de sfr trafic-en avant** niveau de l'interface ; cependant, cette configuration est purement pour la fonctionnalité de démonstration et ne devrait pas être utilisée sur une production ASA. Aucune question qui sont trouvées dans cette caractéristique de démonstration n'est prise en charge par le centre

d'assistance technique Cisco (TAC). Si vous désirez déployer le service ASA SFR en mode passif, configurez-le avec l'utilisation d'un *policy-map*.

4. Spécifiez un emplacement et appliquez la stratégie. Vous pouvez appliquer une stratégie globalement ou sur une interface. Afin d'ignorer la stratégie globale sur une interface, vous pouvez s'appliquer une stratégie de service à cette interface.

   Le mot clé **global** applique la carte de stratégie à toutes les interfaces, et le mot clé d'**interface** s'applique la stratégie à une interface. On permet seulement une stratégie globale. Dans cet exemple, la stratégie est appliquée globalement :

   `ciscoasa(config)# service-policy global_policy global` **Attention** : **Le global_policy de** carte de stratégie est une stratégie par défaut. Si vous utilisez cette stratégie et voulez l'enlever sur votre périphérique pour dépanner des buts, assurez-vous que vous comprenez son implication.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Enregistrez un périphérique avec un centre de Gestion de FireSIGHT
- Déploiement de centre de Gestion de FireSIGHT sur le VMware ESXi
- Scénarios de configuration de Gestion IPS sur un module 5500-X IPS
- Support et documentation techniques - Cisco Systems